| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/644,031 | 08/22/2000 | James P. Cusey | 20661-00818 | 1287 |

7590            04/08/2004

Roger L. Maxwell
Jenkens & Gilchrist P C
1445 Ross Avenue
Suite 3200
Dallas, TX  75202-2799

| EXAMINER |
|---|
| LANIER, BENJAMIN E |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2132 | 5 |

DATE MAILED: 04/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

## Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**.           2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

4)☒ Claim(s) _1-33_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-33_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

## Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _22 August 2000_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All    b)☐ Some * c)☐ None of:

       1.☐ Certified copies of the priority documents have been received.

       2.☐ Certified copies of the priority documents have been received in Application No. _____.

       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _4_.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

1.      The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2.      Claims 13-17, 19, 24-27, 29, 30 are rejected under 35 U.S.C. 102(b) as being anticipated

by Herve, U.S. Patent No. 4,471,216. Referring to claims 13-17, 19, 24-27, 29, 30, Herve

discloses a system for identification of facilities requesters wherein a facility transmits a random

number to devices requesting access (Col. 1, lines 62-65), which meets the limitation of

transmitting and receiving a challenge. The requesting device then applies the random number

along with a secret code (device secret), and an identification code (device ID) in a function to

produce an output (Col. 1, line 66 – Col. 2, line 4), which meets the limitation of generating a

nonreversible computation result, wherein the outputted response to the challenge includes the

nonreversible computation result, and wherein the nonreversible computation result is computed

by seed an algorithm with the received challenge, a device secret, and a unique device identifier.

The facility computes a similar output using the same items and the same function. Upon

reception of the requesting device output, the facility compares the received output with it's own

generated output to authenticate the requesting device (Col. 2, lines 1-4), which meets the

limitation of receiving a response from the device, the response including the result of the

nonreversible computation, which is seeded with at least the challenge, and authenticating the

response from the device.

3.      Claims 1-7, 9, 13-17, 19, 24-27, 29-32 are rejected under 35 U.S.C. 102(b) as being

anticipated by Pieterse, U.S. Patent No. 5,907,832. Referring to claims 1, 4-7, 9, 13-17, 19, 24-

27, 29, 30, Pieterse discloses an electronic payment debiting system wherein a terminal generates

and then transmits to the payment device, a random number (challenge) (Col. 4, lines 35-36),

which meets the limitation of transmitting and receiving a challenge. Based on the random

number the payment device computes an authentication code (Col. 4, lines 47-45) on the random

number (challenge), card balance (device secret), and an identification code (device id)(Col. 7,

lines 9-11) using a hash function (Col. 5, line 54), which meets the limitation computing a

nonreversible computation using the stored device ID, the stored device secret, and a challenge

as seeds. The authentication code is the transmitted to the terminal, the terminal can then

authenticate the code by regenerating and comparing the authentication code (Col. 4, lines 46-

67), which meets the limitation of receiving a response from the device, the response including

the result of the nonreversible computation, which is seeded with at least the challenge, and

authenticating the response from the device. The balance (device secret) is stored in the

EEPROM memory (Fig. 5, Col. 7, lines 3-4), which meets the limitation of a second memory

portion configured to store a device secret. The identification code is stored in dynamic memory

(first memory)(Col. 7, lines 10-14).

        Referring to claims 3, 4, Pieterse discloses that the random number (service provider data

item) is stored in a register (third memory portion)(Col. 7, lines 3-4), and the initialization vector

would be the counter value (Col. 5, lines 61-65).

Referring to claims 31, 32, Pieterse discloses that a debiting command (partial secret) is

received at the device and used to lower the balance (device secret) (Col. 2, lines 60-64), which

meets the limitation of computing the device secret using the partial secret.

*Claim Rejections - 35 USC § 103*

4.      The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

5.      Claims 8, 20-23, 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Pieterse, U.S. Patent No. 5,907,832, in view of Saunders, U.S. Patent No. 5,917,421. Referring to

claims 8, 20-23, 33, Pieterse discloses an electronic payment debiting system wherein a terminal

generates and then transmits to the payment device, a random number (challenge) (Col. 4, lines

35-36), which meets the limitation of transmitting and receiving a challenge. Based on the

random number the payment device computes an authentication code (Col. 4, lines 47-45) on the

random number (challenge), card balance (device secret), and an identification code (device

id)(Col. 7, lines 9-11) using a hash function (Col. 5, line 54), which meets the limitation

computing a nonreversible computation using the stored device ID, the stored device secret, and

a challenge as seeds. The authentication code is the transmitted to the terminal, the terminal can

then authenticate the code by regenerating and comparing the authentication code (Col. 4, lines

46-67), which meets the limitation of receiving a response from the device, the response

including the result of the nonreversible computation, which is seeded with at least the challenge,

and authenticating the response from the device. The balance (device secret) is stored in the

EEPROM memory (Fig. 5, Col. 7, lines 3-4), which meets the limitation of a second memory

portion configured to store a device secret. The identification code is stored in dynamic memory

(first memory)(Col. 7, lines 10-14). Pieterse does not disclose that the system contains a printer.

Saunders discloses an authentication system in the form of an ATM which provides a user with

access to an account and provides the user with a print out of the transactions made (Fig. 1, Col.

1, lines 26-63 & Col. 2, line 28). It would have been obvious to one of ordinary skill in the art at

the time the invention was made to use a printer in the electronic payment debiting system of

Pieterse in order to provide the user a print out of the transactions made during their account

access as taught in Saunders (Col. 2, lines 44-48).

6.      Claims 20-23, 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herve,

U.S. Patent No. 4,471,216, in view of Saunders, U.S. Patent No. 5,917,421. Referring to claims

20-23, 33, Herve discloses a system for identification of facilities requesters wherein a facility

transmits a random number to devices requesting access (Col. 1, lines 62-65), which meets the

limitation of transmitting and receiving a challenge. The requesting device then applies the

random number along with a secret code (device secret), and an identification code (device ID)

in a function to produce an output (Col. 1, line 66 – Col. 2, line 4), which meets the limitation of

generating a nonreversible computation result, wherein the outputted response to the challenge

includes the nonreversible computation result, and wherein the nonreversible computation result

is computed by seed an algorithm with the received challenge, a device secret, and a unique

device identifier. The facility computes a similar output using the same items and the same

function. Upon reception of the requesting device output, the facility compares the received

output with it's own generated output to authenticate the requesting device (Col. 2, lines 1-4),

which meets the limitation of receiving a response from the device, the response including the

result of the nonreversible computation, which is seeded with at least the challenge, and

authenticating the response from the device. Herve does not disclose that the system contains a

printer. Saunders discloses an authentication system in the form of an ATM which provides a

user with access to an account and provides the user with a print out of the transactions made

(Fig. 1, Col. 1, lines 26-63 & Col. 2, line 28). It would have been obvious to one of ordinary skill

in the art at the time the invention was made to use a printer in the system for identification of

facilities requesters of Herve in order to provide the user a print out of the transactions made

during their account access as taught in Saunders (Col. 2, lines 44-48).

7.      Claims 18, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herve, U.S.

Patent No. 4,471,216, in view of Halpern, U.S. Patent No. 4906,828. Referring to claims 18, 28,

Herve discloses a system for identification of facilities requesters wherein a facility transmits a

random number to devices requesting access (Col. 1, lines 62-65), which meets the limitation of

transmitting and receiving a challenge. The requesting device then applies the random number

along with a secret code (device secret), and an identification code (device ID) in a function to

produce an output (Col. 1, line 66 – Col. 2, line 4), which meets the limitation of generating a

nonreversible computation result, wherein the outputted response to the challenge includes the

nonreversible computation result, and wherein the nonreversible computation result is computed

by seed an algorithm with the received challenge, a device secret, and a unique device identifier.

The facility computes a similar output using the same items and the same function. Upon

reception of the requesting device output, the facility compares the received output with it's own

generated output to authenticate the requesting device (Col. 2, lines 1-4), which meets the

limitation of receiving a response from the device, the response including the result of the

nonreversible computation, which is seeded with at least the challenge, and authenticating the

response from the device. Herve does not disclose disabling the card when the comparison fails.

Halpern discloses an electronic fund transfer system that compares data on a central computer

with data from a card. Upon a failed comparison, the card is disabled (Col. 3, line 59 – Col. 4,

line 5). It would have been obvious to one of ordinary skill in the art at the time the invention

was made to disable the card of Herve upon a failed comparison in order to prevent fraudulent

attempts against the system as taught in Halpern (Col. 4, lines 6-9).

8.      Claims 18, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pieterse,

U.S. Patent No. 5,907,832, in view of Halpern, U.S. Patent No. 4906,828. Referring to claims 18,

28, Pieterse discloses an electronic payment debiting system wherein a terminal generates and

then transmits to the payment device, a random number (challenge) (Col. 4, lines 35-36), which

meets the limitation of transmitting and receiving a challenge. Based on the random number the

payment device computes an authentication code (Col. 4, lines 47-45) on the random number

(challenge), card balance (device secret), and an identification code (device id)(Col. 7, lines 9-

11) using a hash function (Col. 5, line 54), which meets the limitation computing a nonreversible

computation using the stored device ID, the stored device secret, and a challenge as seeds. The

authentication code is the transmitted to the terminal, the terminal can then authenticate the code

by regenerating and comparing the authentication code (Col. 4, lines 46-67), which meets the

limitation of receiving a response from the device, the response including the result of the

nonreversible computation, which is seeded with at least the challenge, and authenticating the

response from the device. The balance (device secret) is stored in the EEPROM memory (Fig. 5,

Col. 7, lines 3-4), which meets the limitation of a second memory portion configured to store a

device secret. The identification code is stored in dynamic memory (first memory)(Col. 7, lines

10-14). Pieterse does not disclose disabling the card when the comparison fails. Halpern

discloses an electronic fund transfer system that compares data on a central computer with data

from a card. Upon a failed comparison, the card is disabled (Col. 3, line 59 – Col. 4, line 5). It

would have been obvious to one of ordinary skill in the art at the time the invention was made to

disable the card of Pieterse upon a failed comparison in order to prevent fraudulent attempts

against the system as taught in Halpern (Col. 4, lines 6-9).

9.      Claims 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pieterse,

U.S. Patent No. 5,907,832, in view of Schneier. Referring to claims 10-12, Pieterse discloses an

electronic payment debiting system wherein a terminal generates and then transmits to the

payment device, a random number (challenge) (Col. 4, lines 35-36), which meets the limitation

of transmitting and receiving a challenge. Based on the random number the payment device

computes an authentication code (Col. 4, lines 47-45) on the random number (challenge), card

balance (device secret), and an identification code (device id)(Col. 7, lines 9-11) using a hash

function (Col. 5, line 54), which meets the limitation computing a nonreversible computation

using the stored device ID, the stored device secret, and a challenge as seeds. The authentication

code is the transmitted to the terminal, the terminal can then authenticate the code by

regenerating and comparing the authentication code (Col. 4, lines 46-67), which meets the

limitation of receiving a response from the device, the response including the result of the

nonreversible computation, which is seeded with at least the challenge, and authenticating the

response from the device. The balance (device secret) is stored in the EEPROM memory (Fig. 5,

Col. 7, lines 3-4), which meets the limitation of a second memory portion configured to store a

device secret. The identification code is stored in dynamic memory (first memory)(Col. 7, lines

10-14). Pieterse does not disclose that the hash function is a SHA hash function. Schneier

discloses using SHA hash algorithms as a one-way hash function in cryptographic procedures

(pgs. 442-445). It would have been obvious to one of ordinary skill in the art at the time the

invention was made for the hash function of Pieterse to be a SHA function because Schneier

discloses (page 442) that the SHA function is a standard hashing function.

## *Conclusion*

10.    The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

Pailles, U.S. Patent No. 5,495,098

Van de Pavert, EP 637,004 A1

Pedersen, U.S. Patent No. 5,739,511

11.    Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Benjamin E Lanier whose telephone number is 703-305-7684.

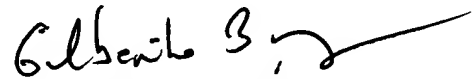The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on (703)305-1830. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100